

Google

[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)

Ring test primality

Search

[Advanced Search](#)  
[Preferences](#)

## Web

Results 1 - 10 of about 63,500 for **Ring test primality**. (0.12 seconds)**AKS Primality Test** -- from Wolfram MathWorld

Lenstra H. W. Jr. and Pomerance C. "Primality Testing with Gaussian Periods." Manuscript. March 2003. Pomerance, C. "The Cyclotomic **Ring Test** of Agrawal, ... mathworld.wolfram.com/AKSPrimalityTest.html - 21k - [Cached](#) - [Similar pages](#)

**Polynomial time deterministic method for testing primality of ...**

In the second stage, **primality** tester 106 performs an "extension **ring test**". Steps 208 to 214 illustrate the extension **ring test**. ...  
www.freepatentsonline.com/20050027764.html - 64k - [Cached](#) - [Similar pages](#)

**[PDF] C:/E/postdoc/Fields & DIMACS/temp/research-at-dimacs.dvi**File Format: PDF/Adobe Acrobat - [View as HTML](#)

that arise from studying the problems of **primality testing**, ... We show that **ring** isomorphism and automorphism problems are not only related to the graph ...  
homepages.cwi.nl/~ns/about-dir/research.pdf - [Similar pages](#)

**An Improved Las Vegas Primality Test** - Kaltofen, Valente, Yui ...

We present a modification of the Goldwasser Kilian Atkin **primality test**, ... Atkin's method computes the order of an elliptic curve whose endomorphism **ring** is ...  
citeseer.ist.psu.edu/kaltofen89improved.html - 22k - [Cached](#) - [Similar pages](#)

**[PDF] On the implementation of AKS-class primality tests**File Format: PDF/Adobe Acrobat - [View as HTML](#)

In previous years there had appeared **primality tests** that "seemed ... Pomerance C 2002, "The cyclotomic **ring test** of Agrawal, Kayal, and Saxena.", preprint. ...  
developer.apple.com/hardware/ve/pdf/aks3.pdf - [Similar pages](#)

**[PS] Lecture 14 1 Review of Factorization 2 Primality testing**File Format: Adobe PostScript - [View as Text](#)

we can describe each **ring** starting with smaller subrings and use a finite number of extensions to describe the entire **ring**. 2 **Primality testing** ...  
theory.csail.mit.edu/~madhu/FT05/scribe/lect14.ps - [Similar pages](#)

**[PDF] 1 Introduction 2 Using properties of  $\mathbb{Z}$  for primality testing**File Format: PDF/Adobe Acrobat - [View as HTML](#)

for **primality testing**. For any number  $n$ , consider the **ring**  $R = \mathbb{Z}_n$ . Recall the following two facts related to  $\mathbb{Z}_n$ . Fact 2.1 If  $n$  is prime, then ...  
www.cse.iitk.ac.in/users/manindra/CS681/Lecture12.pdf - [Similar pages](#)

**[PDF] Rene Schoof Amsterdam, October 16, 2004 Four primality testing ...**File Format: PDF/Adobe Acrobat - [View as HTML](#)

Each **test** involves an exponentiation in the **ring**  $\mathbb{Z}/n\mathbb{Z}$ . Since the exponent is less ... is a polynomial time **primality test**. Testing  $n$  takes  $O((\log n)^3)$  ...  
www.mat.uniroma2.it/~schoof/millerrabinpom.pdf - [Similar pages](#)

**[PDF] An Improved Las Vegas Primality Test \***

File Format: PDF/Adobe Acrobat

isomorphic to the **ring** of integers of a given imaginary ... **primality test** due to Goldwasser and Kilian (1986) was the first of its kind to use elliptic ...  
portal.acm.org/citation.cfm?doid=74540.74545 - [Similar pages](#)

**37a**

A pseudofield is a pair  $(A, \alpha)$  where  $A$  is a **ring** (commutative with ... In the context of **primality testing**, there is a procedure which converts any ...

http://www.google.com/search?hl=en&rls=GGLD%2CGGLD%3A2004-30%2CGGLD%3Aen&q=+Ring... 5/16/2007